

5

## CLAIMS

1. A cryptographic communication system comprising:  
a key distribution server for distributing a key used to  
decrypt encrypted information; and  
10 a specific number of subscriber terminals using said  
information,  
wherein said key distribution server distributes:  
an encrypted first group key used to decrypt said  
information;  
15 individual decryption information corresponding to said  
specific number of subscriber terminals and used to perform  
decryption of said first group key; and  
individual key update information corresponding to said  
specific number of subscriber terminals and used to perform a part  
20 of decryption of a second group key, said second group key being  
updated after a group key is updated,  
and wherein said specific number of subscriber terminals decrypt  
said first group key distributed from said key distribution  
server by use of results obtained by processing operations  
25 performed based on said key update information previously  
obtained and used to decrypt said first group key, as well as by  
use of said decryption information distributed from said key  
distribution server.
- 30 2. The cryptographic communication system according to claim  
1, wherein said specific number of subscriber terminals implement  
a part of decryption of said group key, said decryption being  
performed using said individual key update information, before  
distribution of said group key.
- 35 3. The cryptographic communication system according to claim  
1, wherein said key distribution server distributes to said

5 specific number of subscriber terminals key update information,  
used to decrypt said first group key, together with a third group  
key, said third group key being in a state before said third group  
key gets updated to said first group key.

10 4. The cryptographic communication system according to claim  
1, wherein in the event where said key distribution server updates  
said group key, said key distribution server determines which  
subscriber terminals among said specific number of subscriber  
15 number of subscriber terminals, together with said group key  
being updated, said decryption information used by remaining  
subscriber terminals other than said subscriber terminals to be  
excluded to make said remaining subscriber terminals able to  
decrypt said group key being updated.

20

5. A key distribution server for distributing a key used to  
decrypt encrypted information, comprising:

means for generating a first group key used to decrypt said  
information and encrypting said first group key;

25 means for generating individual decryption information  
used to perform decryption of said first group key and  
corresponding to subscriber terminals;

means for generating individual key update information  
used to perform a part of decryption of a second group key, said  
30 second key being updated after a group key is updated, and  
corresponding to said subscriber terminals; and

means for distributing said first group key, said  
decryption information and said key update information to said  
subscriber terminals.

35

6. The key distribution server according to claim 5, wherein  
said means for generating said decryption information determines

5 which terminals among said subscriber terminals are to be excluded and generates said decryption information used by remaining subscriber terminals other than said subscriber terminals to be excluded in order to make said remaining subscriber terminals able to decrypt said group key.

10

7. A terminal device comprising:

means for retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and decryption information used to decrypt said group key;

15 means for performing a part of decryption of said group key before distribution of said group key; and

means for decrypting said group key by use of results obtained by processing operations performed based on a part of decryption of said group key and said decryption information  
20 retrieved from said key distribution server.

8. A program for controlling a computer and then distributing a key used to decrypt encrypted information, said program making said computer have capabilities including:

25 a function of generating a first group key used to decrypt said information and encrypting said first group key;

a function of generating individual decryption information used to perform decryption of said first group key and corresponding to subscriber terminals;

30 a function of generating individual key update information used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals; and

a function of distributing said first group key, said  
35 decryption information and said key update information to said subscriber terminals via specific communication means.

5     9.     The program according to claim 8, wherein said function of  
generating individual decryption information determines which  
subscriber terminals among said subscriber terminals are to be  
excluded and generates said decryption information used by  
remaining subscriber terminals other than said subscriber  
10    terminals to be excluded in order to make said remaining  
subscriber terminals able to decrypt said group key.

10.    A program for controlling a computer and then achieving a  
specific function, said program making said computer have  
15    capabilities including:

        a function of retrieving from a specific key distribution  
server a group key encrypted to decrypt encrypted information and  
decryption information used to decrypt said group key via  
specific communication means;

20          a function of performing a part of decryption of said group  
key before distribution of said group key; and

        a function of decrypting said group key by use of results  
obtained by processing operations performed based on a part of  
decryption of said group key and said decryption information  
25    retrieved from said key distribution server.

11.    A recording medium recording a program thereon for  
controlling a computer and then distributing a key used to decrypt  
encrypted information, said program being made readable by said  
30    computer so as to make said computer have capabilities achieved  
though use of said program, said program including:

        a function of generating a first group key used to decrypt  
said information and encrypting said first group key;

        a function of generating individual decryption information  
35    used to perform decryption of said first group key and  
corresponding to subscriber terminals;

        a function of generating individual key update information

5 used to perform a part of decryption of a second group key, said second key being updated after a group key is updated, and corresponding to said subscriber terminals; and

10 a function of distributing said first group key, said decryption information and said key update information to said subscriber terminals via specific communication means.

12. A recording medium recording a program thereon for controlling a computer and then achieving a specific function, said program being made readable by said computer so as to make  
15 said computer have capabilities achieved though use of said program, said program including:

20 a function of retrieving from a specific key distribution server a group key encrypted to decrypt encrypted information and decryption information used to decrypt said group key via specific communication means;

a function of performing a part of decryption of said group key before distribution of said group key; and

25 a function of decrypting said group key by making use of results obtained by processing operations performed based on a part of decryption of said group key and said decryption information retrieved from said key distribution server.

13. A key sharing method for making a specific number of terminals share a key used to decrypt encrypted information, said  
30 specific number of terminals making use of said information, said method comprising:

a step of making said specific number of terminals perform a part of decryption of an encrypted group key used to decrypt said information before distribution of said group key;

35 a step of distributing to said specific number of terminals said group key and individual decryption information used to perform a part of remaining decryption other than said part of

5 decryption of said group key and corresponding to said specific  
number of terminals; and

a step of making said specific number of terminals perform  
decryption of said group key using said decryption information  
being distributed and results obtained by performing a part of  
10 decryption of said group key, said part of decryption previously  
being performed.

14. The key sharing method according to claim 13, wherein  
information used to perform said part of decryption is  
15 distributed in advance of distribution of said group key to said  
specific number of terminals together with said group key, said  
group key being in a state before being updated.